

PUBLIC PRIVATE COOPERATION: CHALLENGES AND OPPORTUNITIES IN SECURITY GOVERNANCE

BENJAMIN S. BUCKLAND, THEODOR H. WINKLER



PUBLIC PRIVATE COOPERATION: CHALLENGES AND OPPORTUNITIES IN SECURITY GOVERNANCE

BENJAMIN S. BUCKLAND, THEODOR H. WINKLER





TABLE OF CONTENTS

ABSTRACT	7
INTRODUCTION.....	9
1. DEFINITIONS AND HISTORICAL PERSPECTIVES	12
2. DEMOCRATIC GOVERNANCE CHALLENGES	17
2.1 OVERSIGHT.....	18
2.2 JUDICIAL MEASURES.....	23
2.3 SELF-REGULATION	25
2.4 CONTRACTS	27
CONCLUSIONS.....	31
REFERENCES.....	33
ABOUT THE SERIES	35



ABSTRACT

When faced with both traditional and non-traditional security challenges, states, acting alone, are poorly-equipped. Ad hoc security governance networks have increasingly been the response. Such networks involve cooperation between governments, the private sector, non-governmental and international organisations and enable actors to take advantage of geographical, technological, and knowledge resources they would be unable to muster alone. However, there are many as yet unanswered questions about the oversight and accountability of new governance networks, as well as about ways in which, on the positive side, they can better contribute to improved security. This paper looks at both the challenges and some potential solutions to the democratic governance challenges posed by public private cooperation in the security domain.

INTRODUCTION¹

In 1795, Edmund Burke noted that “one of the finest problems in legislation [is to determine] what the state ought to take upon itself to direct by the public wisdom, and what it ought to leave, with as little interference as possible, to individual discretion.”² It is this problem that has guided debates on privatization ever since, from the large-scale sell-offs of Thatcher’s 1980s Britain, via the Public Private Partnerships of the 1990s, to the ad hoc governance networks of today. While we visit the history of privatisation in a little more detail below, it is worth noting at the outset that here we have tried to avoid ideological debates regarding the relative benefits or deficiencies of neo-liberalism. Instead, this paper takes as a premise two things.

Firstly (and somewhat obviously) that a great deal of privatisation has taken place and regardless of one’s views on its merits, a number of resultant democratic governance challenges remain to be addressed. Secondly, that, when faced with a number of contemporary security challenges, states, acting alone, are poorly-equipped and that, to face these challenges, state involvement in ad hoc security governance networks (often involving private partners) is increasingly necessary.

Challenges such as cyber security are one obvious example of this although others abound. These include pandemics (which require coordinated action by a range of actors including: states, international organisations, such as the WHO, and pharmaceutical companies); non-proliferation of nuclear, biological or chemical weapons (export controls, for example, requiring close industry cooperation); and corruption (effective counter-corruption requiring close cooperation between civil society actors, states, IOs and private firms).

Ad hoc security governance networks required to face these and other contemporary challenges involve cooperation between governments, the private sector, non-governmental and international organisations

¹ The authors would like to thank Liliana Andonova, Anne-Marie Buzatu, Anja Ebnöther, Mark Knight, André du Plessis and Aidan Wills, for their insightful comments and contributions to the text. All photographs are the property of the authors or have been used under a creative commons license from J.D. Mack, ahisgett and Mac(3).

² Cited in William L. Megginson and Jeffry M. Netter, “History and Methods of Privatization,” in *International Handbook on Privatization*, ed. David Parker and David Saal (Cheltenham and Northhampton: Edward Elgar, 2003), 25.

(among others) and enable actors to take advantage of geographical, technological, and knowledge resources they would be unable to muster alone. However, as with what we might call “more traditional” forms of privatisation or outsourcing, they pose many as yet unanswered questions related to transparency oversight and accountability, as well as about ways in which, on the positive side, they can better contribute to improved security.

One feature of these new governance networks is the large and growing role that private actors play within them. Private actors are everywhere. IT companies write the software and build the hardware that allows states to fight against online-crime and wage cyber-war; airlines and shipping companies are increasingly involved in privatised forms of border protection, and migration management; the robotics firms that build drones and military robots write software that finds targets and sets mission priorities; private technicians and weapons experts man ships and military bases; businesses scour open-sources for intelligence on terrorism that they sell to governments.

A great deal of material has been produced on the rise of private military and security companies (PMSCs). Recent work has also sought to integrate these actors into a wider SSR and SSG agenda. However, there is, as yet, very little that takes the logical next step and explores the role of a wider range of private and other non-state actors in responding to a broad range of security governance challenges. We will be obliged in the years to come to broaden our analytical horizons way beyond current SSR and SSG approaches. There is a growing urgency to move beyond the first revolution in this area that led to the “whole of government” approach towards a second revolution, one that leads to a fully integrated security sector approach that reaches beyond established state structures to include select private companies – and thus permit, what we might call, a “whole of issues” approach.

There is nothing inherently wrong with private actors playing a role, even a leading role, in security provision. Indeed, “as long as there is consent and social recognition, an actor – even a private actor – can be accorded the rights, the legitimacy, and the responsibilities of an

authority.”³ However, it does not take much investigation to discover a plethora of examples in which private security “solutions” have turned out to be worse than the threat they were employed to resolve. This is particularly the case when there is an absence of adequate control and oversight or where accountability structures are weak or nonexistent.

The problem is exacerbated when the very existence (and growing role) of a private dimension within an evolving security network is not yet fully recognised and understood by political and parliamentary oversight bodies, let alone by the wider public. A prime example is information technology (IT), in which technological change has long outpaced the state’s ability to regulate, control, and protect a rapidly-developing medium. The fact that IT is a genuinely cross-cutting issue (making the attribution of oversight responsibility difficult, if not impossible) only further amplifies the problem.

While other papers in the Horizon 2015 series look closely at specific actors and issues, the discussion below is quite general in scope. Rather than looking in too much detail at specific examples of public private cooperation – in the running of prisons or the collection of intelligence, for example – we look below at the general problems that such cooperation engenders from a democratic governance perspective, as well as at how some of these problems can be eliminated.

³ Rodney Bruce Hall and Thomas J. Biersteker, eds. *The Emergence of Private Authority in Global Governance* (Cambridge: Cambridge University Press, 2002), 204.

1. DEFINITIONS AND HISTORICAL PERSPECTIVES

As the length of time required to build complex and highly integrated weapons systems grew, their manufacture increasingly required dedicated firms and specialised labour, operating in times of peace as well as war. This production capacity has often been state-owned (in the case of the Venice Arsenal, for example) but it has also involved large-scale public-private cooperation, what in the 20th century has come to be known (following the Farewell Address of President Dwight Eisenhower) as the military industrial complex. Despite its striking effectiveness in producing advanced systems (the leading role of Newport News in US naval shipbuilding springs to mind) the military industrial complex has also proven vulnerable to the principal-agent problem, moral hazard, rent-seeking and political corruption.⁴

In the US, as well as in states with much longer histories of state-owned security industries, the 1980s saw radical waves of privatisation, in which large amounts of formerly-public services and infrastructure were moved into the private sector. Between 1980 and 1992, eighty states launched ambitious privatisation efforts and, in that period, approximately 6,800 state-owned enterprises were privatised, of which around 2,000 were in the developing world.⁵

The United Kingdom (UK) was at the vanguard. In line with promises made before the 1979 election, the Conservative Prime Minister, Margaret Thatcher, worked quickly to denationalise the British armaments industry, selling off firms such as British Aerospace (BAE) and Rolls-Royce, as well as Royal Ordnance Factories and Royal Dockyards.⁶ The government initially retained a “special share” in these firms (in order to maintain democratic control) but this did not give it any role in management or development.⁷ As the 1980s went on, this programme was extended to defence support services, such as catering, cleaning, security guarding,

⁴ Martin Edmonds, “Defence Privatisation: From State Enterprise to Commercialism,” *Cambridge Review of International Affairs* 13, no.1 (1999): 114-129.

⁵ Sunita Kikeri, John R. Nellis and Mary M. Shirley, *Privatization: The Lessons of Experience* (Washington DC: World Bank Publications, 1992), 2.

⁶ Elke Krahmann, *States Citizens and the Privatisation of Security* (Cambridge: Cambridge University Press, 2010), 73-4.

⁷ Idem.

engineering, training, supply and operations support. This pattern was similar to paths taken in the period by governments worldwide. “The delegation of operational decision-making authority for large-scale projects to prime contractors was aimed at reducing management costs, transferring risk, and increasing economic flexibility.”⁸

In general, the arguments made in support of privatisation have been related to efficiency. Indeed, John Moore, the Financial Secretary to the Treasury from 1983 to 1986 in the Conservative government of Margaret Thatcher (and the man responsible for a great deal of the privatisation that went on in the UK during the period) remarked later that:

Begin as a radical experiment, privatisation works so well that it has become a practical process by which a state-owned industry can join the free market with visible, often dramatic gains for the industry, its employees, its customers, and for the citizens who set it free by purchasing its shares.⁹

In Africa, Latin America and in many parts of Asia, development actors, such as the World Bank, supported large-scale privatisation as an essential part of achieving broader goals of economic development and poverty reduction.¹⁰ They argued that freeing state treasuries from the drain placed on them by inefficient, loss-making enterprises, would free up capital and lead to rapid economic gains and improved social welfare.

In recent years, new language that makes reference to “joined up government”, “holistic government”, and public-private cooperation has replaced earlier talk of contracting out and privatization.¹¹ Again, the UK was one of the first places to talk about the idea in its current form, with the then Conservative government introducing its “private finance initiative” in 1992. Under the scheme, private firms would design, build, operate and finance hospitals, prisons, schools, and so forth, to public specifications. The government would agree to purchase the service for a fixed period, after which it would revert to public ownership. When they came to power in 1997, New Labour continued in the same vein but rebranded the idea as “public private partnerships” (PPPs). The idea,

⁸ Idem.

⁹ Cited in Stephen Martin and David Parker, *The Impact of Privatisation: Ownership and Corporate Performance in the UK* (London: Taylor and Francis, 1997), xi.

¹⁰ Kikeri, Nellis and Shirley, *Privatization*, 1.

¹¹ Roger Wettenhall, “The Rhetoric and Reality of Public-Private Partnerships,” *Public Organization Review* 3, (2003), 78.

however, was not even particularly novel in the early nineties. Australia first toyed with “private infrastructure involvement” in the early 1980s. New Zealand adopted wide-ranging reforms under the banner of “new public management.”¹² South Africa and Spain have also been pioneers in the area, adopting similar reforms, “described variously as restructuring, reengineering, divestment, privatization and the adoption of strategic equity partnerships.”¹³

As with earlier waves of privatisation, a key driver of more recent efforts at increasing “public private cooperation” is economic. Governments are seeking to save money as they deal with growing challenges with shrinking resources. Private “manegerialism” has become widely regarded as an antidote to the perceived bureaucracy and inefficiencies of the public sector.¹⁴ Furthermore, debates over issues such as high crime have increasingly concluded that there has been a “theory failure” rather than a mere failure of implementation. Proponents of the theory failure view argue that there is a need for new alliances and new roles for the private sector.¹⁵ There is, of course, mixed evidence on whether privatisation results in increased efficiency or cost-reduction and, in any case, it is clear that “cheaper” is not always a good thing, particularly where security is concerned.¹⁶

Setting aside efficiency questions and economic arguments, it is worth noting that the use of terms such as “privatisation” and “public private partnership” can be misleading, particularly when the discussion turns to the apparently shrinking role of the state.¹⁷ Given the complexity of the processes involved, what is happening needs to be analysed on a case by case basis before conclusions can be drawn.¹⁸ There is a tendency to talk about “traditional” state functions and to use this as a basis for analysis but history reveals the situation to be more complicated. Indeed, some have even argued that it is “not only misleading but indeed dangerous to

¹² Judy Whitcombe, “Contributions and Challenges of ‘New Public Management’: New Zealand Since 1984,” *Policy Quarterly* 4, no.3 (September 2008): 7-13.

¹³ Wettenhall, “The Rhetoric and Reality of Public-Private Partnerships,” 82; Jody Freeman, “The Private Role in Public Governance,” *New York University Law Review* 75, no.3 (2000): 553.

¹⁴ Nik Theodore, Nina Martin and Ryan Hollon, “Securing the City: Emerging Markets in the Private Provision of Security Services in Chicago,” *Social Justice* 33, no.3 (2006): 86.

¹⁵ Idem.

¹⁶ Brian Gran and William Henry, “Holding Private Prisons Accountable: A Socio-Legal Analysis of ‘Contracting Out’ Prisons,” *Social Justice* 34, no.3-4 (2007-8): 176.

¹⁷ Alyson Bayles, “Private Sector, Public Security,” in *Private Actors and Security Governance*, ed. Alan Bryden and Marina Caparini (Geneva: Lit Verlag, 2006), 42.

¹⁸ Bayles, “Private Sector, Public Security,” 42.

the continuing public interest to pedal the view that the role of the state has been diminished or displaced in the new arrangements, which is, of course, what the word ‘privatization’ implies.”¹⁹ “Virtually any example of service provision or regulation reveals a deep interdependence among public and private actors in accomplishing the business of government.”²⁰ Private actors set standards; provide services; deliver benefits; implement, monitor and enforce compliance with regulations; and exert coercive power.²¹

Indeed, when confronting many contemporary challenges – cyber security being an obvious example – arguments over public and private roles are entirely beside the point. To continue with the cyber security example, the constellation of relevant actors will always be both public and private. The idea that Google or Oracle or IBM could or should be state-owned is nonsensical, but their importance to cyber security is unquestionable. In the case of IT security, as with many other contemporary challenges, private and public actors have always been involved and their continued cooperation is essential if the challenge is to be met with any semblance of efficiency or effectiveness. It is the novelty of such cooperation and the scale of its development and impact that make contemporary challenges so unique, that makes our understanding of them so limited and that renders current regulation so inadequate.

Instead, it is perhaps more fruitful to avoid normative discussions about “traditional” roles altogether and instead focus on democratic governance challenges and how to overcome them, regardless of whether they occur in the strictly public or private sphere. Given that private firms (particularly in the security domain) are subject to widely varying levels of government control, the question then becomes about how to improve such control and ensure norms of good governance and accountability are respected.²²

Areas in which private actors are involved include (broadly defined): defence, intelligence gathering, defence (both defensive and offensive military operations), security services, prisons, the financial

¹⁹ Wettenhall, “The Rhetoric and Reality of Public-Private Partnerships,” 82.

²⁰ Freeman, “The Private Role in Public Governance,” 547.

²¹ Idem.

²² Gran and Henry, “Holding Private Prisons Accountable,” 174.

sector and markets, among many others. The boxes in the text provide some examples.

Box 1. Private Military and Security²³

The growth of Private Military and Security Companies (PMSCs) has been substantial in recent years, significantly altering the face of the security sector. The phenomenon is most profound in the anglo-saxon world, where PMSCs have become a multi-billion dollar enterprise. In the US, there exist 2-3 private security guards for every law enforcement officer. The trend has, however, is widespread. Thus, Germany counts today 307 private security guards per 100'000 inhabitants (versus 327 police personnel), while the corresponding figures for Sweden are 182 and for Spain 165.

The problem is, though, not only one of numbers, but rather of a much more fundamental nature. Which state functions can be outsourced to PMSCs and which cannot? What minimal regulatory standards are required? What licensing procedures should apply? What training requirements should be imposed for what job? How can transparency, public responsibility and accountability be assured? What form of cooperation between private and public agencies is necessary and what sort of cooperation should be precluded?

These questions become ever more urgent as, increasingly, there is a division, increasingly, between state run investigations and counterforce, and private-run patrols and visible crime prevention, the latter being comparatively poorly trained and poorly paid. From a democratic governance perspective, a perhaps more worrying development is the fact that a large number of "grey" or "hybrid" bodies with both public and private status are also emerging. Private guards are increasingly being drawn (in the UK, for example) into public functions, where they are granted legal powers. Furthermore, PMSCs now play an ever increasing role in military operations and risk there to render parliamentary oversight and public scrutiny ever more difficult. Tragedies such as the now infamous Nisour Square incident, involving the US PMSC "Blackwater" (now Xe Services) have further highlighted the problems of respect of human rights and accountability posed by different rules and practices of engagement.

²³ L. Johnston, "Private Policing: Uniformity and Diversity," in *Policing Across The World: Issues for the Twenty-First Century*, ed. R. I. Mawby (London: Routledge, 1998); Theodore, Martin and Hollon, "Securing the City," 89; Theodore, Martin and Hollon, "Securing the City," 89.

2. DEMOCRATIC GOVERNANCE CHALLENGES

Regardless of the security domain in which private actors are active, the question of their accountability – of whom, to whom, by what – is among the most pressing from a democratic governance point of view. At its heart, it is about responsibility, although this responsibility may be vis-à-vis a range of different actors, including to the users of a service, to the organisation that contracted them to perform, to their shareholders or other stakeholders, to industry or trade associations, as well as to oversight bodies, such as relevant parliamentary committees or ombuds institutions.²⁴

The proliferation of private activity in the security domain means there is less justification than ever for ring-fencing security industries and excluding them from transparency processes, external oversight, corporate governance and competition.²⁵ Private actors are one step further removed from direct accountability to the electorate and to democratic institutions. They are vulnerable to private actions in tort or contract cases, subject to anti-trust law, and subject to agency oversight, but nevertheless they escape most of the procedural controls and budgetary constraints that apply to government agencies. They are often insulated from the legislative, executive, and judicial oversight that agencies must submit to. Furthermore, they have different goals and respond to a wide range of different incentives.²⁶ Accountability failures can thus be attributed to both governmental failures to develop and implement sound accountability policies. But also to the fact that private firms have a large number of competing accountability demands, relationships and obligations, not all of which are equal in strength.²⁷ If contracts are well written and oversight is diligent, private actors can be held to higher standards than even public bodies but this is, unfortunately, more often the exception than the rule.

²⁴ David Bull, "Private Prisons and Public Accountability," *Journal of Sociology* 36, no.2 (August 2000): 270.

²⁵ Bayles, "Private Sector, Public Security," 47.

²⁶ Freeman, "The Private Role in Public Governance," 574.

²⁷ Harald Bergsteiner and Gayle C. Avery, "A Generic Multiple Constituency matrix: Accountability in Private Prisons," *Journal of Public Administration Research* 19, (2008): 649.

Finally, it is worth pointing out that, in the case of public private cooperation, there is a need for a combination of both formal and informal accountability mechanisms. Indeed, the fact that formal government oversight exists does not mean that something is accountable, just as the participation of private actors in an aspect of security governance does not automatically mean it is unaccountable. The following sections, on oversight, on legal measures, on self-regulation and on contracts, explore some of the mechanisms by which accountability and transparency can be maintained during public private cooperation. It is far from an exhaustive list but hopefully it does something to illustrate the range of policy options available, as well as highlight the importance of their goal.

Box 2. Private Intelligence²⁸

It may be true that some private involvement in intelligence gathering is essential. Agencies need the cooperation of telecommunications and IT firms to establish wiretaps and monitor communications. In addition, the procurement and continuing operation of high-tech equipment, such as spy satellites, may only be possible through public private cooperation. While very little information is available on the precise nature of intelligence privatisation, outside of the US, it seems clear that it is a growing industry in many parts of the world, particularly since September 11.

Simon Chesterman, in one of the few articles published on the issue, suggests that the US spent 70 percent (roughly 42 billion USD) of its 2005 intelligence budget on private contractors. Furthermore, he reports that private contractors outnumber their public colleagues at the Pentagon's Counterintelligence Field Activity unit, at the Defence Intelligence Agency, in the CIA's National Clandestine Service and at the National Counterterrorism Center. These contractors are involved in all aspects of intelligence gathering, including covert operations. To give just one example, the British firm Aegis, now based in Switzerland, was awarded in 2004 a 300 million USD contract which required the hiring of a team of analysts with "NATO equivalent SECRET clearance."

This aspect of public private cooperation raises many familiar questions regarding oversight and accountability. Contractor involvement in intelligence activities often shields such activity from scrutiny by oversight bodies, as well as leading to conflicts of interest when commercial and operational priorities collide.

2.1 OVERSIGHT

Oversight can be divided into three categories: executive oversight, parliamentary oversight, and non-political oversight. Due to the wide scope of public private cooperation, executive oversight and or control over a private security partner may vary enormously. A government department may, for example, purchase open-source intelligence information from

²⁸ Simon Chesterman, "'We Can't Spy ... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions,'" *The European Journal of International Law* 19, no.5 (2008): 1055-6; Chesterman, "'We Can't Spy ... If We Can't Buy!', 1058; Chesterman, "'We Can't Spy ... If We Can't Buy!', 1054-74; Mark Mazzetti, "U.S. Still Using Private Spy Ring, Despite Doubts," *The New York Times*, May 15, 2010.

a private firm over which it has no control or oversight at all. On the other hand, a ministry with responsibility for prisons, for example, may be able to control and oversee everything down to the smallest details of a private firm's operations. Of course, it is important that the executive is not too closely involved in the minutiae of a private actor's operations – beyond the setting of certain minimum standards related, for example, to respect for human rights and the rule of law. In doing so, it would become impossible for them to act as a source of external control and the basis of democratic oversight would thus be undermined.²⁹

In addition from their legislative role, parliaments perform a crucial role in scrutinising government actions. Indeed is is the very essence of democratic societies that parliaments are able to investigate all areas of state activity, particularly those related to security. With regards to public private cooperation, parliamentary oversight must guarantee legitimacy and democratic accountability by ensuring that the activities of both public and private actors: serve the interests of the state (rather than narrow political or sectoral interests); conform to minimum standards related, for example, to human rights protection and international law; are in line with a state's overall strategic interests; and meet established standards of financial probity and transparency. In general, parliamentary oversight will be exercised through a specialised body (often a parliamentary committee).³⁰

Non-political oversight generally takes the form of complaints systems, auditors general, auditors and ad hoc oversight by civil society and media. Independent offices, such as inspectors general, judicial commissioners or auditors have been set up in a number of states and given statutory access to information and staff, in order that they can oversee aspects of the security sector. Depending on their status, inspectors general can report to any of the three branches of government and may be asked to review an agency's performance against one or more of several standards: efficiency, compliance with government policies or targets, propriety or legality.³¹ In some states, such as Australia, they also have jurisdiction to deal with individual complaints. Auditors, on the other hand, will generally report on questions of legality and efficiency

²⁹ Hans Born and Ian Leigh, "Democratic Accountability of Intelligence Services" (DCAF Policy Paper, no.19, 2007), 6-7.

³⁰ Ibid., 10-11.

³¹ Ibid., 18-19.

of expenditure, on possible irregularities and on whether a service has operated within or exceeded its budget.³²

A number of factors make oversight particularly difficult in the case of public private cooperation. These are explored below.

First, oversight challenges are exacerbated by network complexity. As is illustrated below, a large and diverse number of state, private, international and other non-state actors are involved in security provision. Network complexity makes it difficult for oversight bodies, such as parliamentary committees (with often limited capacity), to keep track of relevant actors, to gain knowledge of their existence and activities or even to acquire a legal mandate to do so. The problem is amplified by new security networks that transcend established parliamentary committee borders and oversight responsibilities. One thus needs to ask both: is there accountability, transparency, control, as well as (the more worrying question) of whether parliamentary oversight bodies even aware of their existence/functions?

Second, oversight challenges are increased by technical complexity. Because of the highly technical nature of many security challenges and responses, oversight bodies often lack the required expertise and highly specialised staff to understand and adequately oversee them. Public private cooperation exacerbates the problem by creating a divide between the highly paid and sophisticated technical experts involved in implementing a directive and the (often) poorly paid and less well informed government actors charged with their oversight.

Third, oversight challenges are compounded by legal complexity. This complexity relates, above all, to questions of jurisdiction and to questions regarding responsibility and control. In particular, private security firms are both willing and able to transform or relocate in order to circumvent local regulations. This is particularly problematic when we consider that many relevant operations take place in failed or troubled states: states in which the regulatory environment is often completely inadequate. A related issue is that even in relatively competent states the resources required to detect and report on the overseas activities of

³² Idem.

a private security partner based in their territory are often prohibitively expensive.³³

Fourth, oversight challenges are reinforced by the heterogeneity of actors involved. In most instances, oversight institutions are organised along agency or functional lines. For example, a parliamentary committee may oversee intelligence services and activities, the armed forces, or justice. Public private security cooperation, however, often cuts across agency boundaries and thus across areas of oversight mandate. The result is a large number of areas in which there is no or inadequate oversight or (at the very least) substantial overlap and confusion with respect to the question of who is, on the basis of what law, in charge of what.

Fifth, oversight challenges are amplified by mandate perceptions. In general, government oversight bodies are concerned with the government agencies over which they have direct responsibility. This leaves the private partners of such agencies out of the reach of oversight, even in cases where they are directly funded by, or work in close collaboration with such agencies.

Sixth, oversight challenges are exaggerated by the breaking of principal/agent bonds. The actions of every government agent are connected in a chain of responsibility from principal to agent. For example, a Paris police officer is linked via his or her superiors to the prévôt (the senior officer in the force), to the prefect (the politically appointed head of the force) and, ultimately, to the interior ministry and the executive. There is thus a link of responsibility and oversight between instruments of democratic governance (such as the parliament) and individuals or agencies carrying out government directives. These links are severed by the introduction of private actors and the creation of public private cooperation mechanisms. While a publicly contracted security firm may seem to act as a simple agent of the state (the principal), the relationship is generally much more complex and clouded by numerous information asymmetries that reduce transparency and prevent oversight mechanisms from operating effectively. This problem is further multiplied if private actors contracted by a government hire, in turn, private sub-contractors. To unravel the resulting tangle of contractual obligations and to establish

³³ Ibid, 536.

clear lines of accountability surpasses the capacity of most oversight bodies.

Finally, oversight challenges are intensified by competing obligations and possible conflicts of interest that may arise when private security firms are staffed by former high officials as is often the case. Similarly, it is important that monitoring be used to ensure that state officials are not “captured” (through corruption or other means) by the organisations they are meant to be supervising.³⁴

Box 3. Defence Procurement³⁵

The defence sector has often involved large-scale public-private cooperation. Indeed, the sector is probably the oldest example of such cooperation in the security domain – giant firms like Boeing, Newport News, McDonnell Douglas and many others have been (in various incarnations) dominant actors on the US security landscape for over a century. In consequence, private involvement here is relatively familiar and generally regarded as of little concern. Nevertheless, as an increasing number of defence technologies are dual use or “multivalent”, the problem emerges of how to effectively stop them from spreading into the wrong hands, particularly when the proliferation of dual use products is combined with the multiplication of new firms not necessarily bound by existing contracts or codes of conduct. Export controls are another possible regulatory instrument and have worked well in areas such as nuclear proliferation (via the forty-six member Nuclear Suppliers Group). They have been less effective, however, in regards to technology that is more widespread, as is the case, for example, with chemical and biological agents.

The problem obtains a much more fundamental dimension when, as today, technological change is no longer driven by the military industrial complex but by private and civilian industries. A concern is that, if states lose control of security-relevant technology, their ability to counteract threats leads inexorably towards further reliance on private actors, which, in turn, further reduces state capacity. Having outsourced high-tech capabilities to the private sector, it is often very difficult (if not impossible) to re-establish control should it one day be necessary. In a perfect example of this problem, the US Navy recently signed a 3.3 billion dollar no-bid contract with IT firm Hewlett-Packard, designed to let the Navy wean itself off reliance on the firm over five years. This contract is the (hopefully) final step in a process that began in 2008 when, after many years and many billions of dollars, the Navy declared that it would reassess control over its IT networks. However, it soon became apparent that this was more difficult than it first appeared.

Military leaders wondered whether they had the expertise to manage such a complex IT project. Contractors working on the Navy’s behalf shared those concerns. The Navy might be able to build an aircraft carrier, say. But those ships take a decade or more to build. Something as fast moving as IT? That requires a different metabolism, a different workforce and a different set of skills. Then there was the question of intellectual property. HP owned all of NMCI’s designs. Without that information, the Navy couldn’t really begin to plan for the Navy’s Next Generation Enterprise Network, or NGEN. (The new network had to be based on the old one, after all.) Which meant the military needed yet another agreement with Hewlett-Packard if they ever hoped to separate from the company. “Without access to the infrastructure and technical data associated with NMCI, we can’t hold an open competition.”

As one Department of the Navy civilian told a journalist for Wired magazine, “HP is holding the Navy hostage, and there isn’t a peep about it. We basically had two recourses: pay, or send in the Marines.”

³⁴ Bull, “Private Prisons and Public Accountability,” 270.

³⁵ Megan Bastick, “The Role of Penal Reform in Security Sector Reform” (DCAF Occasional Paper, no.18, 2010), 19.

2.2 JUDICIAL MEASURES

Private actors are involved in the provision of a great number of security-related activities. Some of these services are uncontroversial, while others provoke a great deal of debate, including active engagement in hostilities, guard services (particularly in military prisons), interrogation services, intelligence gathering, training and other disarmament demobilisation and reintegration (DDR) tasks, among many others. The possibility that private actors may not be subject to the same national and international legal standards (or that they may conduct their activities in territories or foreign countries where those standards are not applicable or cannot be enforced) as their government counterparts is one of the key reasons for this controversy. Indeed, “any use of a private intermediary blocks the way to the normal exercise of democratic controls … that have been designed for state … activity [in addition] it makes the application of domestic and international laws more difficult and sometimes impracticable.”³⁶

While implementation may be lacking in practice, a large number of regulatory and executive solutions are available, on paper at least. These include: licensing of corporations, export controls (on goods and services), corporate transparency requirements, laws on punishment of illegal activities committed abroad, stricter contracts (see below), legal frameworks, standard-setting, monitoring, black-lists, and better identification and enforcement of relevant international norms.³⁷ Of these, the regulatory components can be divided into three broad types: general guidelines for conduct (for example, the Swiss Initiative, which produced the Montreux Document outlining International Humanitarian Law [IHL] standards as they relate to PMSCs), criminalisation of certain behaviour (for example, the South African law on PMSCs), and cultivation of the legitimate market (for example, market incentives causing Blackwater to change its name to Xe Services).³⁸

One constant problem, however, is related to jurisdiction and, in particular, to what one might call “the disengagement of law and state.”

³⁶ Bayles, “Private Sector, Public Security,” 48; August Reinisch, “Securing The Accountability of International Organizations,” *Global Governance* 7, (2001): 133.

³⁷ Bayles, “Private Sector, Public Security,” 49.

³⁸ Simon Chesterman, “Blackwater and the Limits to Outsourcing Security,” *The New York Times*, November 12, 2009.

Firstly, it may be difficult to determine the nationality of an international corporation. Secondly, even where nationality is clear, it is not always the case that the overseas actions of a company will fall under the jurisdiction of a local court. Where this is the case, courts in the country of operation can sometimes fill the void, although this is unlikely in many conflict or post-conflict states, where institutions are weak and (often) unwilling or unable to challenge foreign firms.

Box 4. Private prisons³⁹

Since the early 1990s, there has been a revival in the contracting of prison labour. In the US, for example, prison labour is now a 1.4 billion dollar industry. This, along with the outsourcing of the prisons themselves, constitutes what me might call a "double privatisation."

In terms of democratic oversight, the key roles are played by parliament and by the judiciary, which together develop and interpret penal standards and conduct inquiries into conditions or specific events within individual prisons or the system as a whole. They are joined by civil society actors, many of whom have a strong tradition of involvement in prison-related advocacy.

However, these more traditional oversight bodies and mechanisms have been joined in many states by a second group of actors. As a result of privatisation, prisons in Australia, Canada and the US, as elsewhere now form part of a subgovernmental network of government agencies, corporations, and professional associations. All of which have a role in law-making, norm formation and standard-setting. Professional associations – the American Corrections Association (ACA) in the US, for example – play a huge role. Indeed, the ACA manual plays a greater role than government authority in establishing prison standards and in transforming vague directives (against, for example, "cruel and unusual punishment") into specific operational terms. Nevertheless, there remain doubts, both with respect to the proper implementation of those standards as well as with regards to the question of whether such a sensitive dimension of the security sector should belong into private hands at all.

For the most serious of crimes or for crimes falling into a specific legal category, international or regional courts – such as the European Court for Human Rights (ECtHR) may offer a solution. Some American and Commonwealth courts have also, in some limited cases, sought to impose constitutional requirements on private actors, and subjected their decisions to judicial review, although others (the US Supreme Court being a notable example) have seemed very reluctant to go in this direction.⁴⁰

Finally, there is the possibility that some tasks should never be outsourced at all. Interrogation and covert intelligence gathering are two examples that may be appropriate here. Firstly because, for some of the reasons outlined above, outsourcing makes effective accountability

³⁹ Noel Shachtman, "HP Holds Navy Network 'Hostage' for \$3.3 Billion," *Wired Magazine*, August 31, 2010.

⁴⁰ Freeman, "The Private Role in Public Governance," 575–6.

difficult and, in some cases, impossible. Secondly, even when it may be necessary to push the limits of the law to deal with major threats (as some have argued is the case when confronting transnational terrorist organisations), such action can only be justified (if ever) if it takes place within a democratic framework. These questions are clearly of far more weight than those related to cost and efficiency.⁴¹

2.3 SELF-REGULATION

Codes of conduct and the development of industry standards can play an important role. From the point of view of the state, they can help to increase transparency and serve as a yardstick against which performance and practice can be measured and judged. From the point of view of the private actor, they can serve to codify what each player in an interdependent market can expect from one another. This can be very attractive, particularly where failure or negligence on the part of one actor can have system-wide effects (as is the case, for example, with IT security).

The ability of a self-regulatory body to be effective depends on a number of factors, including: formal supervision, internal structures, institutional background, vulnerability of individual actors to poor publicity) and peer pressure.⁴² Visible industries, for obvious reasons, have greater incentives to develop self-regulatory mechanisms and enforce compliance with their rules.

In addition to informal and voluntary self-regulation, states sometimes mandate private actors to act as regulators and set and implement standards, subject to a degree of government oversight.⁴³ Securities exchanges and broker dealers are two examples (from outside the security domain) that self-regulate in this manner.

Government involvement (even in industry-led standard setting) can help to improve enforcement.⁴⁴ In the same way, third parties can improve accountability. To take just one example, mandatory disclosure (of performance statistics, for example) can then be subject to oversight

⁴¹ Chesterman, "Blackwater and the Limits to Outsourcing Security."

⁴² Freeman, "The Private Role in Public Governance," 649.

⁴³ Idem.

⁴⁴ Intelligence and National Security Alliance, *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models* (Arlington VA: INSA, 2009), 7.

and monitoring by third-party auditors and experts. Banks and insurance firms can sometimes act as third-party regulators, given their interest in protecting the value of investments.

While self-regulation can be a partial solution, however, current examples reveal major enforcement problems. Many trade associations, for example, have never expelled a member for non-compliance and, furthermore, self-regulatory bodies also often lack transparency and public involvement. And, while the threat of government imposed standards can be a spur to better self-regulation, powerful self-regulatory bodies can supplant the role of the state – acting as a powerful deterrent to legislation, should the state later decide it is necessary.⁴⁵

Trends towards greater privatisation of regulation, however, will always be problematic given the limited accountability of private firms. Such arrangements can also lead to concerns about the anti-competitive effects of allowing private actors to police themselves.⁴⁶ Indeed, self-regulatory bodies have been called “networked oligopolies, with unprecedented power to extract regulatory concessions from host governments.”⁴⁷ Dispersal of authority can also be attractive to governments, given that it may allow them to escape blame, should problems occur.⁴⁸ This is particularly worrying given that private accreditation often leaves little recourse for damaged parties when the system fails.⁴⁹

A slight variation on self-regulation (which avoids some of its more obvious problems) is what has been called the “reg-neg” approach. This involves consultation with stakeholders followed by government regulation. Such a consensus-based approach can gain wide traction but may also be problematic given that it involves the partial surrender of rule-making power to interest groups. It thus has the potential to be undemocratic and produce undesirable outcomes.⁵⁰ Because enforcement is rarely perfect, especially in complex topic areas, such as security, implementation always involves cooperation. The problem is how to ensure that it is forthcoming. Ultimately, each context requires specific

⁴⁵ Freeman, “The Private Role in Public Governance,” 647.

⁴⁶ Ibid., 650.

⁴⁷ Bierstecker and Hall *The Emergence of Private Authority in Global Governance*, 211.

⁴⁸ Ibid., 212.

⁴⁹ Freeman, “The Private Role in Public Governance,” 613.

⁵⁰ Freeman, “The Private Role in Public Governance,” 655–6.

analysis to determine the best method of ensuring accountability and compliance.

Box 5. The Kimberley Process and the EITI⁵¹

The Kimberley Process Certification Scheme entered into force in 2003 after a landmark United Nations General Assembly Resolution in November 2000. It is designed to certify the origin of rough diamonds from sources which are free of conflict and halt the trade in so-called “blood diamonds.”

A large number of similar initiatives exist, covering domains as diverse as the diamond industry (in the case of the Kimberley Process) and internet privacy and freedom of expression (in the case of the Global Network Initiative). Many have had notable successes, the Kimberley Process has led to improved regulation in many states and the Extractive Industries Transparency Initiative (EITI) has led to increased oversight and accountability. In addition, corporations have benefited from the good publicity that stems from cooperation with civil society.

All of these initiatives stem from the idea that voluntary standard-setting, monitoring and verification can help tackle specific problems. But, in many cases, questions have come to be raised about whether the interests of individual members will always end up undermining the consensus approach.

In 2008, a massacre in Zimbabwe’s Marange diamond fields left 200 people dead. Despite calls for Zimbabwe to be suspended from the Kimberley Process as a result, moves were blocked by other states party. As a compromise, it was agreed that exports from Marange would be suspended, although it has now emerged that they continued until mid-2010. Global Witness, an advocacy group, says that a failure to act is fundamentally undermining the scheme. This failure raises a broader question about the success and utility, not only of the Kimberley Process itself, but of similar initiatives worldwide.

As Graham Baxter remarked, with regards to the Kimberley Process, “Initially, there was a flush of enthusiasm that government, business and civil society could really grab the ball and run with it ahead of regulation but now the question is, is this approach really working?” Similar worries exist regarding the Voluntary Principles on Security and Human Rights and the Extractive Industries Transparency Initiative (EITI). Both have had big problems, particularly with enforcement.

2.4 CONTRACTS

Contracts are involved to a greater or lesser extent in almost every area of public-private cooperation in the security domain. They are essential to ensuring accountability, transparency and good practices. Indeed, given how difficult it may be to hold private actors accountable (to human rights and IHL norms, for example), contracts may be the only means of ensuring compliance with procedural and substantive standards that might be otherwise inapplicable or unenforceable.⁵²

⁵¹ Hugh Williamson, “Stakeholder Coalitions in Crisis,” The Financial Times, June 7, 2010; Graham Baxter cited in Williamson, “Stakeholder Coalitions in Crisis.”

⁵² Freeman, “The Private Role in Public Governance,” 634; Gran and Henry, “Holding Private Prisons Accountable,” 177.

The number of things that can be specified in a contract is endless. A contract between a state and a security provider, for example, might conceivably include articles on: procedural and oversight requirements (such as compliance with government regulations related to administrative procedures or freedom of information); minimum employee training standards; background checks; performance payments and fines; information exchange; compliance; monitoring processes; standards; liability; conduct; whether a mix of public and private employees is required; what (if any) involvement of independent (for example, human rights) groups might be appropriate; monitoring and independent review; and grievance systems.

One difficulty in formulating contract provisions is that they need to be specific enough to enable monitoring and accountability but flexible enough that private firms can adapt to changing conditions, find efficiencies and seek out opportunities for improvement, without which there are few benefits to privatisation in the first place.

Aside for questions of pure content, it is crucial that initial contracts are strong, given that it is often hard for the public to wrestle back control after it has been given up. This is particularly the case given that (in contrast with regulation) the judiciary is unlikely to defer to government in interpretation or permit them to unilaterally amend contractual terms.⁵³ Similarly, without enforcement, detailed contract provisions are meaningless, particularly where they leave room for wide interpretation.

Some activities leave little room for discretion in that they are fairly easy to specify precisely in a contract. Provision of meals at a military base might be one example. But there are many others, particularly related to security, that are not easily reduced to contractual obligations or, at least not in ways that don't leave wide scope for interpretation and discretion. Such activities are difficult to "prevent through delineated delegation or to police without formal oversight mechanisms."⁵⁴ Such activities result in considerable sharing of discretionary authority between public and private actors, even though the public will often retain the ability to impose conditions and have ultimate responsibility.

⁵³ Freeman, "The Private Role in Public Governance," 670.
⁵⁴ Ibid., 597.

Something that creates serious accountability problems and obstacles to meaningful oversight is the fact that few opportunities or incentives exist for the public to monitor private security providers. To take one example, that of private prisons, the low status of those incarcerated is a further barrier. Furthermore, prisons “confer on private actors a powerful combination of policy making, implementation, and enforcement authority in a setting rife with the potential for abuse.”⁵⁵ Many situations are hard to specify contractually and conflicts of interest, incentives and opportunities to cut costs exist in ways that are hard to detect and monitor and “harder still to press in a human rights action.”⁵⁶

Furthermore, there are an increasingly large number of examples of public private cooperation in which the relationship is one of equals and more horizontal than vertical, something that restricts opportunities for democratic oversight. One recent example of this phenomenon is the agreement between Google and the US National Security Agency (NSA), apparently to help the search giant shore up its networks and identify recent attackers.⁵⁷ Director of National Intelligence, Admiral Dennis Blair, argued, with relevance to the Google attack, that cyberspace could not be secured without a “collaborative effort that incorporates both the US private sector and our international partners.”⁵⁸ However, civil society groups, such as the Electronic Privacy Information Center (EPIC) have raised concerns about a lack of transparency and oversight, EPIC’s Executive Director Marc Rotenberg commenting that “We can’t afford to have secret cybersecurity policy that impacts the privacy rights of millions of internet users.”⁵⁹

While contracts may play an important role in the oversight of public-private cooperation, there is a need for both formal and informal mechanisms, involving both government supervision, as well as independent third parties, and firms themselves. Independent third parties (such as public interest or professional associations) play important roles in implementation through compliance monitoring and acting as private attorneys general in several regulatory settings.⁶⁰ Third

⁵⁵ Ibid., 632.

⁵⁶ Idem.

⁵⁷ Kim Zetter, “Google Asks NSA to Help Secure Its Network,” *Wired*, February 4, 2010.

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ Freeman, “The Private Role in Public Governance,” 551.

parties, particularly the public and civil society actors can also play a role in contract-making, lending legitimacy to the process. They can also help by developing “model” contracts or by creating codes of conduct that can be appended to contracts in specific areas.

Contracting can, counter-intuitively, increase government control in some circumstances – when written well, a contract can allow a state to enforce antidiscrimination law or environmental standards, for example, in areas where regulation may not otherwise be clearly applicable.⁶¹ This assumes, however, that state agencies don’t become dependent on the firms to whom they have contracted out services; their bargaining power can diminish over time as private actors gain a monopoly on the services they deliver or as the state’s administrative oversight capacity is reduced.⁶²

Box 6. Corruption⁶³

An underlying assumption behind a great deal of security-related outsourcing is that it is cheaper and that private firms are more nimble and better at finding savings than huge military bureaucracies. However, the reduction in oversight, that is characteristic of much outsourcing, increases opportunities for corruption, undermining the cost and efficiency argument.

There is an abundance of examples. In Iraq, for example, Parsons Global Services Inc. lost a contract to build 150 health centres after completing only six and collecting 190 million USD – 30 percent more than the original budget. The US Government Accountability Office (GAO) has found that the Pentagon recovered 2 billion USD between 2001 and 2006 from contractors and procurement officials accused of dishonesty or mismanagement and the Special IG for Iraq Reconstruction has eighty open investigations, of which twenty have been referred to the Department of Justice for prosecution.

In similar cases elsewhere, a troubling phenomenon has been the use of national security as a way of halting investigations, despite the fact that economic or national security arguments are not permitted by the OECD bribery convention. Furthermore, most parties to the OECD convention have little or no enforcement mechanisms, beyond peer pressure from other states party. Even where laws are in place, the level of resources allocated to investigation and prosecution is also often worryingly low.

⁶¹ Ibid., 568.

⁶² Idem.

⁶³ Anonymous, “When Outsourcing Turns Outrageous,” BusinessWeek, July 31, 2006; Benjamin W. Heineman Jr. and Fritz Heimann, “Arrested Development: The Fight Against International Corporate Bribery,” The National Interest, (November/ December 2007): 82.

CONCLUSIONS

Arguments about privatisation have often focused on questions of efficiency. The great waves of privatisation that took place in the 1980s and 90s were driven largely by the belief that private actors could deliver services more quickly and more cheaply than their government counterparts. Two things, however, make such arguments largely irrelevant to this paper. Firstly, there are an increasing number of security domains in which public private cooperation is unavoidable, regardless of one's views on its efficiency or otherwise. Cyber security is an obvious example here. Secondly, the involvement of private actors in security-related activities is now so well-established (and indeed essential to the successful accomplishment of many security tasks) that calling for the state to (re)assert ownership is, in many areas, completely unrealistic. Public private security cooperation may be an old phenomenon but it is now a growing one and its implications have not yet been fully grasped by either the institutions directly involved or the bodies that seek to oversee them.

Given these points, it is timely to focus on the challenges that public private cooperation in the security domain raises for democratic governance and, more specifically, on some of the ways that those problems can be mitigated. Private actors are one step further removed from direct accountability to the electorate and to democratic institutions. They are vulnerable to private actions in tort or contract cases, subject to anti-trust law, and subject to agency oversight, but nevertheless they escape most of the procedural controls and budgetary constraints that apply to government agencies. They are often insulated from the legislative, executive, and judicial oversight that agencies must submit to. Furthermore, they have different goals and respond to a wide range of different incentives.⁶⁴

A range of different instruments are available for those wishing to limit the accountability, transparency and oversight deficits created by public private cooperation. Contracts, for example, may be the only means of ensuring compliance with procedural and substantive standards that might be otherwise inapplicable or unenforceable. Self-regulatory

⁶⁴ Freeman, "The Private Role in Public Governance," 574.

mechanisms can also play a role, although their effectiveness depends on a number of factors, including: formal supervision, internal structures, institutional background, the vulnerability of individual actors to poor publicity, and peer pressure.⁶⁵

Similarly, while implementation may be lacking, a large number of regulatory and executive solutions are available. These include: licensing of corporations, export controls (on goods and services), corporate transparency requirements, laws on punishment of illegal activities committed abroad, stricter contracts, legal frameworks, standard-setting, monitoring, black-lists, and better identification and enforcement of relevant international norms.⁶⁶

Parliamentary oversight can be used to limit democratic governance deficits, although, as we saw above, it faces formidable challenges when dealing with non-state bodies and with new types of cooperation. Finally, there needs to be a discussion on what should perhaps never be privatised. While arguments have, thus far, largely focused on the economic, the discussion above suggests that it needs to focus far more on governance deficits and on the areas in which they simply cannot be overcome.

"Where business is part of the problem, it also needs to be part of the solution."⁶⁷ While it is, as yet unclear just what this solution will look like, it is hoped that the discussion above points us in the right direction.

⁶⁵ Freeman, "The Private Role in Public Governance," 649.

⁶⁶ Bayles, "Private Sector, Public Security," 49.

⁶⁷ Ibid., 53.

REFERENCES

- Anonymous, "When Outsourcing Turns Outrageous," *BusinessWeek*, July 31, 2006.
- Bastick, Megan. "The Role of Penal Reform in Security Sector Reform." DCAF Occasional Paper, no.18, 2010.
- Bayles, Alyson. "Private Sector, Public Security." In *Private Actors and Security Governance*, edited by Alan Bryden and Marina Caparini. Geneva: Lit Verlag, 2006.
- Bergsteiner, Harald and Gayle C. Avery. "A Generic Multiple Constituency matrix: Accountability in Private Prisons." *Journal of Public Administration Research* 19, (2008).
- Born, Hans and Ian Leigh. "Democratic Accountability of Intelligence Services." DCAF Policy Paper, no.19, 2007.
- Bull, David. "Private Prisons and Public Accountability." *Journal of Sociology* 36, no.2 (August 2000).
- Chesterman, Simon. "'We Can't Spy ... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions.' *The European Journal of International Law* 19, no.5 (2008).
- Chesterman, Simon. "Blackwater and the Limits to Outsourcing Security." *The New York Times*, November 12, 2009.
- Edmonds, Martin. "Defence Privatisation: From State Enterprise to Commercialism." *Cambridge Review of International Affairs* 13, no.1 (1999).
- Freeman, Jody. "The Private Role in Public Governance." *New York University Law Review* 75, no.3 (2000).
- Gran, Brian and William Henry. "Holding Private Prisons Accountable: A Socio-Legal Analysis of 'Contracting Out' Prisons." *Social Justice* 34, no.3-4 (2007-8).
- Hall, Rodney Bruce. and Thomas J. Biersteker, eds. *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press, 2002.
- Heineman Jr., Benjamin W. and Fritz Heimann. "Arrested Development: The Fight Against International Corporate Bribery." *The National Interest*, (November/December 2007).
- Intelligence and National Security Alliance. *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*. Arlington VA: INSA, 2009.
- Johnston, L. "Private Policing: Uniformity and Diversity." In *Policing Across The World: Issues for the Twenty-First Century*, edited by R. I. Mawby. London: Routledge, 1998.
- Kikeri, Sunita, John R. Nellis and Mary M. Shirley. *Privatization: The Lessons of Experience*. Washington DC: World Bank Publications, 1992.

Krahmann, Elke. *States Citizens and the Privatisation of Security*. Cambridge: Cambridge University Press, 2010.

Martin, Stephen and David Parker. *The Impact of Privatisation: Ownership and Corporate Performance in the UK*. London: Taylor and Francis, 1997.

Mazzetti, Mark. "U.S. Still Using Private Spy Ring, Despite Doubts." *The New York Times*. May 15, 2010.

Megginson, William L. and Jeffry M. Netter. "History and Methods of Privatization." In *International Handbook on Privatization*, edited by David Parker and David Saal. Cheltenham and Northhampton: Edward Elgar, 2003.

Reinisch, August. "Securing The Accountability of International Organizations." *Global Governance* 7, (2001).

Shachtman, Noel. "HP Holds Navy Network 'Hostage' for \$3.3 Billion." *Wired Magazine*, August 31, 2010.

Theodore, Nik, Nina Martin and Ryan Hollon. "Securing the City: Emerging Markets in the Private Provision of Security Services in Chicago." *Social Justice* 33, no.3 (2006).

Wettenhall, Roger. "The Rhetoric and Reality of Public-Private Partnerships." *Public Organization Review* 3, (2003).

Whitcombe, Judy. "Contributions and Challenges of 'New Public Management': New Zealand Since 1984." *Policy Quarterly* 4, no.3 (September 2008).

Williamson, Hugh. "Stakeholder Coalitions in Crisis." *The Financial Times*, June 7, 2010.

Zetter, Kim. "Google Asks NSA to Help Secure Its Network." *Wired*, February 4, 2010.



ABOUT THE SERIES

A great deal of material has been produced on the rise of private military and security companies (PMSCs). Recent work has also sought to integrate these actors into a wider SSR and SSG agenda. However, there is, as yet, very little that takes the logical next step and explores the role of a wider range of private and other non-state actors in responding to a broad range of security governance challenges. We will be obliged in the years to come to broaden our analytical horizons way beyond current SSR and SSG approaches. There is a growing urgency to move beyond the first revolution in this area that led to the “whole of government” approach towards a second revolution, one that leads to a fully integrated security sector approach that reaches beyond established state structures to include select private companies – and thus permit, what we might call, a “whole of issues” approach.

This project brings together relevant state and non-state actors for a series of thematic roundtables throughout 2010. Each roundtable is designed to inform a subsequent working paper. These working papers provide a short introduction to the issue, before going on to examine theoretical and practical questions related to transparency oversight, accountability and democratic governance more generally. The papers, of course, do not seek to solve the issues they address but rather to provide a platform for further work and enquiry. As such, they ask many more questions than they answer. In addition to these working papers, the project has published an occasional paper – *Trends and Challenges in International Security: An Inventory* – that seeks to describe the current security landscape and provide a background to the project’s work as a whole.



The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is the world's leading institution in the areas of security sector reform and security sector governance. DCAF provides in-country advisory support and practical assistance programmes, develops and promotes appropriate democratic norms at the international and national levels, advocates good practices and conducts policy-related research to ensure effective democratic governance of the security sector.

Visit us at: www.dcaf.ch

DCAF Geneva
P.O. Box 1360
1211 Geneva 1
Switzerland

Tel: +41 (22) 741 77 00
Fax: +41 (22) 741 77 05

DCAF Brussels
Place du Congrès 1
1000 Brussels
Belgium

Tel: +32 (2) 229 39 66
Fax: +32 (2) 229 00 35

DCAF Ljubljana
Dunajska cesta 104
1000 Ljubljana
Slovenia

Tel: +386 (1) 5609 300
Fax: +386 (1) 5609 303

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

DCAF Beirut
P.O. Box 113 - 6041
Beirut
Lebanon

Tel: +961 (1) 738 401
Fax: +961 (1) 738 402